REMARKS

Upon entry of this amendment, elected claims 13-16 are all the claims pending in the application. Applicants note that non-elected claims 1-12 and 17-19 have been canceled.

I. Foreign Priority

Applicants note that the present application claims priority under 35 U.S.C. 119. The Examiner, however, has not acknowledged the claim for priority or acknowledged receipt of the certified copies of the priority documents. Accordingly, Applicants kindly request that the Examiner acknowledge the claim for foreign priority and confirm that the certified copies of the priority documents have been received.

II. Information Disclosure Statements

Applicants note that the Examiner has not returned the PTO-1449 forms submitted with the Information Disclosure Statements filed on February 28, 2002 and May 24, 2002. Applicants kindly request that the Examiner consider the references listed on the above-noted PTO-1449 forms and return the initialed and signed forms with the next Office paper.

III. Claim Rejections under 35 U.S.C. § 102

Claims 13 and 14 were rejected under 35 U.S.C. § 102(b) as being anticipated by Schneck et al. (U.S. 6,314,409).

Initially, regarding this rejection, Applicants note that the Examiner inadvertently indicated on page 3 of the Office Action that claims 13 and 14 are rejected under 35 U.S.C. § 103(a), rather than indicating that claims 13 and 14 are rejected under 35 U.S.C. § 102(b).

Regarding claim 13, Applicants note that this claim recites the features of key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, wherein a cryptographic processing means restrains the result of the cryptographic processing from being outputted when the notification signal indicates that key generation is being performed. Applicants respectfully submit that Schneck does not disclose or suggest such features.

Regarding Schneck, Applicants note that this reference discloses a digital data access and distribution system 100 which includes a data distributor 102 and a user 104 (see Fig. 1 and col. 9, lines 51-55). In Schneck, an authoring mechanism 112 provided within the distributor 102 takes data 106 to be packaged and produces packaged data 108, which is sent to the user 104 via a communication channel 105 (see Fig. 1; col. 9, lines 59-64 and col. 11, lines 57-61).

In this regard, as explained with reference to Fig. 4 of Schneck, which shows a flow chart of a version of the authoring mechanism 112, the distributor 102 selects a data-encrypting algorithm (step S400) and a data-encrypting key K_D (step S402), encrypts the data-encrypting key K_D using a rule-encrypting key K_R (step S404), and stores the encrypted key K_D in the encrypted ancillary information 126 of the packaged data 108 (see S406) (see col. 12, lines 29-38).

After storing the encrypted key K_D, each element of the data is examined (step S407), wherein if it is determined that the current data element being examined is in the body of the data, it is then determined in step S410 whether or not the current element is to be protected or not (see col. 13, lines 1-10). If the current data element being examined is not to be protected, it

is stored in the unencrypted body part 122 of the packaged data (step S412), and if it is determined that the current element is to be protected, it is encrypted using the data-encrypting key K_D and then stored in the encrypted body part 120 of the packaged data 108 (step S414).

Further, in another embodiment of Schneck, as explained with reference to Fig. 7, if it is the first time that an access mechanism 114 of the user device 104 is processing rules, then a rule-encrypting key K_R must be determined (step S740), wherein the rule-encrypting key K_R is used for encrypting the data-encrypting key K_D and for encrypting the rules (step S746) (see col. 14, lines 43-62).

As noted above, claim 13 recites the feature of key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not.

In the Office Action, the Examiner has indicated that Schneck discloses the above-noted feature in Fig. 4 and in col. 14, lines 43-61. Applicants respectfully disagree.

In particular, based on the foregoing description of Schneck, Applicants note that while Fig. 4 shows that a data-encrypting key K_D is encrypted using a rule-encrypting key K_R (step S404) and a current data element is analyzed to determine whether it is to be protected or not (step S410), and that col. 14, lines 43-61 indicates that a rule-encrypting key K_R can be calculated (step S740) which is used for encrypting the data-encrypting key K_D and access rules, that such disclosure does not in any way correspond to a key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not.

In view of the foregoing, Applicants respectfully submit that claim 13 is patentable over Schneck, an indication of which is kindly requested. If the Examiner maintains the position that Schneck discloses such a feature, Applicants kindly request that the Examiner explicitly identify the signal disclosed in Schneck which allegedly corresponds to the "notification signal" as recited in claim 13.

Further, as noted above, claim 13 also recites that a cryptographic processing means restrains the result of the cryptographic processing from being outputted when the notification signal indicates that key generation is being performed. In the Office Action, the Examiner has taken the position that Fig. 10A of Schneck discloses this feature (see Office Action at page 3). Applicants respectfully disagree.

Regarding Fig. 10(a) of Schneck, Applicants note that this figure relates to the accessing operation performed by the access mechanism 114 of the user device 104, wherein the user 104 obtains packaged data 108 from the distributor 102 and accesses the data according to the rules provided therewith (see col. 17, lines 46-52). In particular, as explained with reference to Fig. 10(a), it is determined whether a data element is protected (step S1012), wherein if the data element is determined to be protected, then it is next determined whether access to the data element is permitted (step S1014). If access is permitted, then the data element is made available (step S1018), and if no access is permitted, then an access denial operation is performed (step S1016) (see col. 18, lines 44-59).

Thus, while Fig. 10(a) of Schneck depicts the ability to determine whether access to a data element is permitted or not, and deny access if it is determined that access is not permitted

(step S1016), Applicants respectfully submit that this ability does not relate to cryptographic processing means which restrains the result of the cryptographic processing from being outputted when the notification signal indicates that key generation is being performed, as recited in claim 13. In this regard, Applicants note that "the notification signal" recited herein is the notification signal that is output by the key generation means, as discussed above.

In view of the foregoing, Applicants respectfully submit that Schneck does not disclose, suggest or otherwise render obvious the above-noted features of key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, wherein a cryptographic processing means restrains the result of the cryptographic processing from being outputted when the notification signal indicates that key generation is being performed, as recited in claim 13.

Accordingly, Applicants submit that claim 13 is patentable over Schneck, an indication of which is kindly requested.

Regarding claim 14, Applicants note that this claim recites the features of key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, and selection means for selecting a content which is inputted to the cryptographic processing means when the notification signal indicates that key generation is being performed, and otherwise selecting the result of the cryptographic processing outputted from the cryptographic processing means.

As noted above, Schneck discloses that a data-encrypting key K_D is encrypted using a rule-encrypting key K_R (step S404) and a current data element is analyzed to determine whether it is to be protected or not (step S410), a rule-encrypting key K_R that can be calculated (step S740) which is used for encrypting the data-encrypting key K_D and access rules, and the ability to determine whether access to a data element is permitted or not, and deny access if it is determined that access is not permitted (step S1016).

Applicants respectfully submit, however, that such disclosure does not correspond to the above-noted features of key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not, and selection means for selecting a content which is inputted to the cryptographic processing means when the notification signal indicates that key generation is being performed, and otherwise selecting the result of the cryptographic processing outputted from the cryptographic processing means, as recited in claim 14.

Therefore, Applicants respectfully submit that Schneck does not disclose, suggest or otherwise render obvious all of the features recited in claim 14. Accordingly, Applicants submit that claim 14 is patentable over Schneck, an indication of which is kindly requested.

IV. Claim Rejections under 35 U.S.C. § 103(a)

Claims 15 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneck et al. (U.S. 6,314,409) in view of Maytas et al. (U.S. 5,200,999).

Claim 15 recites the feature of key generation means for generating a key with which to apply cryptographic processing to the content and outputting a notification signal which indicates whether key generation is being performed or not.

In the Office Action, the Examiner has taken the position that Schneck discloses such a feature at col. 14, lines 43-61 and in Fig. 4 (see Office Action at page 4). For at least similar reasons as discussed above with respect to claim 13, Applicants respectfully disagree and submit that Schneck does not disclose, suggest or otherwise render obvious such a feature. Further, Applicants submit that Maytas fails to cure this deficiency of Schneck.

In addition, Applicants note that claim 15, as amended, recites the features of input means, to which a content containing an identification signal indicating whether or not to perform cryptographic processing is inputted, for controlling outputting of the inputted content; and cryptographic processing means for applying cryptographic processing to the content outputted from the input means in accordance with the identification signal by using the key, and for outputting a result of the cryptographic processing, wherein the cryptographic processing means outputs to the input means an input enable signal indicating either one of an input enabled state in which inputting of the content from the input means is enabled and an input disabled state in which inputting of the content from the input means is disabled, wherein, when the notification signal indicates that key generation is being performed, the cryptographic processing means outputs to the input means the input enable signal indicating the input disabled state, and wherein the input means disables outputting of the inputted content when the input enable signal indicates the input disabled state.

Applicants respectfully submit that the combination of Schneck and Maytas does not teach or suggest the above-noted features.

In particular, regarding Schneck, as discussed above, this reference discloses that a data-encrypting key K_D is encrypted using a rule-encrypting key K_R (step S404) and a current data element is analyzed to determine whether it is to be protected or not (step S410), a rule-encrypting key K_R that can be calculated (step S740) which is used for encrypting the data-encrypting key K_D and access rules, and the ability to determine whether access to a data element is permitted or not, and deny access if it is determined that access is not permitted (step S1016). Applicants respectfully submit, however, that Schneck does not disclose or in any way suggest the above-noted features recited in amended claim 15.

Regarding Maytas, Applicants note that this reference discloses a cryptographic facility 30 that is maintained within a secure boundary 140 (see Fig. 14 and col. 17, lines 41-43). As shown in Fig. 14 of Maytas, a cryptographic facility access program (CFAP) 34 is coupled to the cryptographic facility 30, wherein the CFAP 34 outputs input parameters to the cryptographic facility 30, and wherein the input parameters are output as output parameters to the CFAP 34 (see col. 17, lines 59-61).

Further, in Fig. 15 of Maytas, it is disclosed that the cryptographic facility 30 incorporates a key record encrypt algorithm and a key record decrypt algorithm, wherein the key record encrypt algorithm 12 includes low level functions used to encrypt a key record and produce an encrypted key authenticator record (KAR), and the key record decrypt algorithm 13 decrypts the encrypted KAR and compares the recovered value of KAR and the generated or produced KAR

for equality in order to determine if the key record has been successfully authenticated (see col. 18, lines 40-42 and lines 52-57; and col. 19, lines 46-57).

Thus, while Maytas discloses the use of an encrypt algorithm 12 and a decrypt algorithm 13, as discussed above, Applicants respectfully submit that Maytas does not disclose or in any way suggest the above-noted features recited in amended claim 15.

In view of the foregoing, Applicants respectfully submit that the combination of Schneck and Maytas does not teach, suggest or otherwise render obvious the above-noted features recited in amended claim 15. Accordingly, Applicants submit that claim 15 is patentable over the cited prior art, an indication of which is kindly requested.

Regarding claim 16, Applicants note that this claim has been amended to recite the features of input means, to which a content containing an identification signal indicating whether or not to perform cryptographic processing is inputted, for controlling outputting of the inputted content; and cryptographic processing means for applying cryptographic processing to the content outputted from the input means in accordance with the identification signal by using the key, and for outputting a result of the cryptographic processing, wherein the key generation means outputs to the input means an input enable signal indicating either one of an input enabled state in which inputting of the content to the cryptographic processing means is enabled and an input disabled state in which inputting of the content to the cryptographic processing means is disabled, wherein, when key generation is being performed, the key generation means outputs to the input means the input enable signal indicating the input disabled state, and wherein the input

means disables outputting of the inputted content when the input enable signal indicates the input disabled state.

Applicants respectfully submit that the combination of Schneck and Maytas does not teach or suggest the above-noted features.

Regarding Schneck, as discussed above, this reference discloses that a data-encrypting key K_D is encrypted using a rule-encrypting key K_R (step S404) and a current data element is analyzed to determine whether it is to be protected or not (step S410), a rule-encrypting key K_R that can be calculated (step S740) which is used for encrypting the data-encrypting key K_D and access rules, and the ability to determine whether access to a data element is permitted or not, and deny access if it is determined that access is not permitted (step S1016). In addition, regarding Maytas, as discussed above, this reference discloses the use of an encrypt algorithm 12 and a decrypt algorithm 13.

Applicants respectfully submit, however, that the combination of Schneck and Maytas does not teach, suggest or otherwise render obvious the above-noted combination of features recited in amended claim 16. Accordingly, Applicants submit that claim 16 is patentable over the cited prior art, an indication of which is kindly requested.

V. Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited.

If any points remain in issue which the Examiner feels may best be resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Mutsuyuki OKAYAMA et al.

By: Kenneth W. Fields

Kenneth W. Fields
Registration No. 52,430
Attorney for Applicants

KWF/jjv
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
February 20, 2007